

Comparison of mixed quantum states

Shengshi Pang and Shengjun Wu

*Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics,
University of Science and Technology of China, Hefei, Anhui 230026, China*

(Dated: September 8, 2011)

In this article, we study the problem of comparing mixed quantum states: given n unknown mixed quantum states, can one determine whether they are identical or not with an unambiguous quantum measurement? We first study universal comparison of mixed quantum states, and prove that this task is generally impossible to accomplish. Then, we focus on unambiguous comparison of n mixed quantum states arbitrarily chosen from a set of k mixed quantum states. The condition for the existence of an unambiguous measurement operator which can produce a conclusive result when the unknown states are actually the same and the condition for the existence of an unambiguous measurement operator when the unknown states are actually different are studied independently. We derive a necessary and sufficient condition for the existence of the first measurement operator, and a necessary condition and two sufficient conditions for the second. Furthermore, we find that the sufficiency of the necessary condition for the second measurement operator has simple and interesting dependence on n and k . At the end, a unified condition is obtained for the simultaneous existence of these two unambiguous measurement operators.

PACS numbers: 03.67.-a, 42.50.Dv, 03.65.Wj, 03.65.Ca, 03.65.Fd

I. INTRODUCTION

Quantum identification problems such as discrimination of quantum states [1–7] and discrimination of quantum operations (or quantum channels) [8–12] are to determine the identity of an unknown quantum state (or quantum channel) chosen from a given set. They have attracted broad interest and received intensive research on the realization conditions and the optimal implementation schemes, due to their key roles in some important quantum information problems like quantum dense coding [13, 14] and so on.

In recent years, a new problem relevant to quantum identification, namely quantum state comparison, has become a new focus of interest in the field of quantum information. Comparison of quantum states is to find out whether several unknown quantum states are identical or not. The reason that it receives much attention is that it has been found especially useful in some interesting quantum verification applications such as quantum fingerprinting [21, 22] and quantum digital signatures [23–25].

The quantum state comparison problem seems similar with quantum state identification at first sight, for if the unknown states can be identified or discriminated, then one can immediately know whether they are identical or different, but it is essentially different from the quantum state identification problem: quantum state comparison only requires to find whether the unknown states are the same or not but not the exact identity of each unknown state, so it is not a must to employ a quantum state identification protocol generally and, what's more, quantum state comparison is usually a non-local operation and can be performed on all the unknown states simultaneously.

So far, universal and unambiguous comparison of pure quantum states has been studied in [15–19], and optimization of the measurement strategy is considered in [16, 18]. Comparison of quantum states has already been realized in experiments [20]. Moreover, comparison of quantum operations and quantum channels has also been investigated in recent research [26–28].

The previous researches on the quantum state comparison problem have been largely focused on pure quantum states, and in this article, we aim to study the comparison of mixed quantum states.

We shall study two types of the quantum state comparison problem in this work. The first type is the universal comparison of mixed quantum states, formulated as follows: given n arbitrary unknown mixed quantum states ρ_1, \dots, ρ_n , is it possible to determine whether they are the same state or not? The second type is the unambiguous comparison of mixed quantum states chosen from a finite set: given n unknown mixed quantum states ρ_1, \dots, ρ_n arbitrarily chosen from a finite fixed set consisting of k mixed states σ_i ($i = 1, \dots, k$) (any state in the set is allowed to be chosen multiple times), can one determine whether they are identical or not by an unambiguous quantum measurement? “Unambiguous” means that the measurement may produce an inclusive result, but if the result is conclusive it must be correct. For succinctness, the set of k mixed states $\{\sigma_i\}_{i=1}^k$ will be called *candidate set*, and the states σ_i ($i = 1, \dots, k$) will be called *candidate states*. The study of unambiguous comparison of mixed states will be based on a *non-trivial condition* which is presented in Sec. II.

In this article, we shall first study the universal comparison of unknown mixed quantum states, and show that this task is impossible to be achieved, in contrast to the universal comparison of pure quantum states which is “half achievable” [16] (the meaning of “half achievable” will be clear in Sec. III). Next, we shall study the unambiguous comparison of unknown mixed quantum states chosen from a given state set. This problem consists of two parts: the possibility to obtain a conclusive result from an unambiguous quantum measurement when the unknown states are actually the same and the possibility to obtain a conclusive result from an unambiguous quantum measurement when the unknown states are actually different. It will be shown that the conditions to realize these two possibilities are different. For the first possibility, we derive a necessary and sufficient condition, and for the second, we obtain a necessary condition and two sufficient conditions.

It is worth mentioning that in earlier researches on quantum comparison of pure states, the main interest was in the condition of realizing the first possibility. In this paper, we not only find a perfect necessary and sufficient condition for the first possibility, but also get fruitful results for the second. For instance, intuitively, the realizability of quantum state comparison should have some dependence on the number of states to be compared and the number of candidate states, but no such result was obtained in any previous literature. However, in our research on the second possibility, we derive such an interesting result. Moreover, in previous researches, the conditions for the two cases were separate and independent of each other, but in our article, we shall establish a unified necessary and sufficient condition for realizing both possibilities simultaneously.

II. PRELIMINARY

Let us begin to present our work with the definitions of some notations used in this paper. We assume that all states lie in a Hilbert space \mathcal{H} of finite dimension d throughout this article. We shall use the *positive operator-valued measure* (POVM) formalism to describe a comparison process. Generally, a POVM representation of a physical

process consists of a series of positive operators corresponding to possible outcomes of the physical process, and these positive operators must sum up to the identity operator. In our research, we shall use M_1 to denote the POVM element which indicates that the n states are identical, M_2 to denote the POVM element which indicates that the n states are different, and an additional operator $M_?$ to denote the POVM element which represents the inconclusive result. Note that $M_?$ will only occur in the unambiguous comparison of quantum states. We shall also use M_1 , M_2 and $M_?$ to represent the corresponding measurement outcomes occasionally if no unambiguity occurs in the contexts. The probability that M_i occurs is

$$\text{Prob}(M_i) = \text{Tr}(M_i \rho_1 \otimes \cdots \otimes \rho_n), \quad \forall i = 1, 2, ?. \quad (1)$$

Throughout this article, we assume that the n states are possessed simultaneously so that collective measurements can be performed on the whole n states, and thus all the measurement operators M_i , $i = 1, 2, ?$, act on the composite Hilbert space $\mathcal{H}^{\otimes n}$.

In addition, we shall use $\text{Supp}(\mathcal{O})$ to denote the support of an operator \mathcal{O} , $\text{Supp}^\perp(\mathcal{O})$ to denote the subspace orthogonal to $\text{Supp}(\mathcal{O})$ in \mathcal{H} , and \mathcal{O} can be a density operator or a more general Hermitian operator. And $\sum_i \text{Supp}(\mathcal{O}_i)$ will be used to denote the subspace spanned by the supports of several \mathcal{O}_i , i.e.

$$\sum_i \text{Supp}(\mathcal{O}_i) = \left\{ \sum_i \vec{v}_i \mid \forall \vec{v}_i \in \text{Supp}(\mathcal{O}_i) \right\}.$$

It can be seen that the measurements like $M_1 = 0$ or $M_2 = 0$ can serve as trivial schemes for unambiguous comparison of mixed quantum states. Obviously this kind of measurement should not be considered, so it is appropriate to require that the conclusive result corresponding to M_1 (or M_2) must occur with a non-zero probability *for at least one group of n states*, and we call this condition as *non-triviality condition*. This condition will be held throughout this article.

III. UNIVERSAL COMPARISON OF MIXED STATES

Our first result is devoted to universal comparison of mixed quantum states. Universal comparison of quantum states concerns with states arbitrarily chosen from the whole Hilbert space \mathcal{H} . In the problem of universal comparison of pure quantum states, it is known that it is impossible to produce an unambiguous result with non-zero probability when the n states are the same but possible when the n states are different [15–17], i.e. M_1 does not exist but M_2 exists (and this is why we said universal comparison of pure states was “half achievable” in Sec. I). However, when the states to be compared are mixed, we show below that it is also impossible to produce an unambiguous comparison result when the states are different, i.e. M_2 does not exist for universal comparison of mixed quantum states.

Theorem 1. Universal comparison of unknown mixed quantum states is impossible.

Proof. We only need to prove that M_2 vanishes in the case of mixed quantum states. Suppose M_2 exists for distinguishing different mixed quantum states universally, then

$$\text{Tr}(M_2 \rho_1 \otimes \rho_2 \otimes \cdots \otimes \rho_n) = 0 \quad (2)$$

when $\rho_1 = \rho_2 = \cdots = \rho_n$ due to the unambiguity of M_2 .

Now we select arbitrary n pure states $|\psi_1\rangle, \dots, |\psi_n\rangle$ from the Hilbert space \mathcal{H} , and let

$$\rho_1 = \rho_2 = \cdots = \rho_n = \frac{1}{d} (|\psi_1\rangle\langle\psi_1| + \cdots + |\psi_n\rangle\langle\psi_n|). \quad (3)$$

Then

$$\text{Prob}(R_2) = \text{Tr}(M_2 \rho_1 \otimes \rho_2 \otimes \cdots \otimes \rho_n) = \frac{1}{d^n} \text{Tr}\left(M_2 (|\psi_1\rangle\langle\psi_1| + \cdots + |\psi_n\rangle\langle\psi_n|)^{\otimes n}\right) = 0. \quad (4)$$

Eq. (4) can be rewritten as

$$\sum_{i_1, \dots, i_n=1}^n \text{Tr}(M_2 |\psi_{i_1}\rangle\langle\psi_{i_1}| \otimes \cdots \otimes |\psi_{i_n}\rangle\langle\psi_{i_n}|) = 0. \quad (5)$$

Since $|\psi_{i_1}\rangle\langle\psi_{i_1}| \otimes \cdots \otimes |\psi_{i_n}\rangle\langle\psi_{i_n}|$ is an n -partite density operator, we have

$$\text{Tr}(M_2 |\psi_{i_1}\rangle\langle\psi_{i_1}| \otimes \cdots \otimes |\psi_{i_n}\rangle\langle\psi_{i_n}|) \geq 0, \quad (6)$$

thus, with Eq. (5), there must be

$$\text{Tr}(M_2|\psi_{i_1}\rangle\langle\psi_{i_1}| \otimes \cdots \otimes |\psi_{i_n}\rangle\langle\psi_{i_n}|) = 0 \quad (7)$$

for all $i_1, i_2, \dots, i_n = 1, \dots, n$. Considering $|\psi_1\rangle, \dots, |\psi_n\rangle$ are arbitrarily chosen from the Hilbert space \mathcal{H} , it can be concluded that $M_2 = 0$. ■

Theorem 1 exhibits the difference between the universal comparison of pure quantum states and that of mixed quantum states. For pure quantum states, when they are the same the comparison measurement can never give any conclusive result, and when they are different the comparison measurement is possible to give a conclusive result with non-zero probability. However, for mixed quantum states, the universal comparison is always impossible.

IV. UNAMBIGUOUS COMPARISON OF MIXED STATES FROM A FINITE SET

In the previous section, we studied universal comparison of mixed quantum states and showed that the task was impossible to accomplish. In the following, we shall turn our attention to unambiguous comparison of unknown mixed quantum states ρ_1, \dots, ρ_n selected from a finite set $\{|\sigma_i\rangle\}_{i=1}^k$. We divide this problem into two parts and study them separately: the possibility to produce an unambiguous result when the n mixed states are actually the same (i.e. the existence of M_1) and the possibility to produce an unambiguous result when the n mixed states are actually different (i.e. the existence of M_2), as we shall see that the results for these two possibilities are quite different.

We first study the first part, i.e. the existence of M_1 . In the following theorem, we show what condition the k candidate states $\sigma_1, \dots, \sigma_k$ should satisfy in order that an unambiguous result can be produced when the n states to be compared are identical.

Theorem 2. For unambiguous comparison of mixed quantum states, a conclusive result can be produced with a non-zero probability when the n states are actually the same, i.e., a non-trivial M_1 exists, if and only if

$$\text{Supp}(\sigma_i) \not\subseteq \sum_{j \neq i} \text{Supp}(\sigma_j), \quad \exists i \in \{1, \dots, k\}. \quad (8)$$

Proof. We first prove the “only if” part by contradiction. Assume that $\text{Supp}(\sigma_i) \subseteq \sum_{j \neq i} \text{Supp}(\sigma_j)$ for all $i = 1, \dots, k$ and let $\rho_1 = \dots = \rho_n = \sigma_i$. Since $\text{Supp}(\sigma_i) \subseteq \sum_{j \neq i} \text{Supp}(\sigma_j)$, we can always find positive coefficients $\alpha_1, \dots, \alpha_{i-1}, \alpha_{i+1}, \dots, \alpha_k$ such that

$$\sum_{j \neq i} \alpha_j \sigma_j - \sigma_i \geq 0, \quad (9)$$

where “ \geq ” means semi-definite positive. Then we have

$$\text{Tr}\left(M_1\left(\sum_{j \neq i} \alpha_j \sigma_j - \sigma_i\right) \otimes \sigma_i \otimes \cdots \otimes \sigma_i\right) \geq 0, \quad (10)$$

or equivalently

$$\sum_{j \neq i} \text{Tr}\left(M_1 \alpha_j \sigma_j \otimes \sigma_i \otimes \cdots \otimes \sigma_i\right) \geq \text{Tr}\left(M_1 \sigma_i \otimes \cdots \otimes \sigma_i\right). \quad (11)$$

According to the unambiguity of the measurement, we have

$$\text{Tr}(M_1 \sigma_j \otimes \sigma_i \otimes \cdots \otimes \sigma_i) = 0, \quad \forall j \neq i. \quad (12)$$

Thus the left side of Eq. (11) is equal to 0 and

$$\text{Tr}(M_1 \sigma_i \otimes \cdots \otimes \sigma_i) \leq 0, \quad \forall i = 1, \dots, k. \quad (13)$$

On the other hand, $\text{Tr}(M_1 \sigma_i \otimes \cdots \otimes \sigma_i) \geq 0$, so it leads to

$$\text{Tr}(M_1 \sigma_i \otimes \cdots \otimes \sigma_i) = 0, \quad \forall i = 1, \dots, k. \quad (14)$$

Note that when ρ_1, \dots, ρ_n are arbitrary different states from the set $\{|\sigma_i\rangle\}_{i=1}^k$, the unambiguity of the measurement gives

$$\text{Tr}(M_1 \rho_1 \otimes \dots \otimes \rho_n) = 0. \quad (15)$$

From (14) and (15), it can be inferred that $M_1 = 0$. Therefore the assumption $\text{Supp}(\sigma_i) \subseteq \sum_{j \neq i} \text{Supp}(\sigma_j)$ for all $i = 1, \dots, k$ is false, and Eq. (8) must be satisfied.

Now we prove the “if” part of the theorem. Suppose $\text{Supp}(\sigma_{i_0}) \not\subseteq \sum_{j \neq i_0} \text{Supp}(\sigma_j)$ for some $i_0 \in \{1, \dots, k\}$, it is easy to see that for each state one can determine whether it is σ_{i_0} or not by local measurements: let $\text{Proj}\left(\sum_{j \neq i_0} \text{Supp}(\sigma_j)\right)^\perp$ denote the projector onto the subspace orthogonal to $\sum_{j \neq i_0} \text{Supp}(\sigma_j)$, then

$$\text{Tr}\left(\sigma_l \text{Proj}\left(\sum_{j \neq i_0} \text{Supp}(\sigma_j)\right)^\perp\right) \neq 0$$

only when $\sigma_l = \sigma_{i_0}$. So, let

$$M_1 = \text{Proj}^{\otimes n}\left(\sum_{j \neq i_0} \text{Supp}(\sigma_j)\right)^\perp, \quad (16)$$

then M_1 will produce a conclusive result when all the n states are all σ_{i_0} . ■

It is worth mentioning that Proposition 1 in Ref. [18] also gives the necessary and sufficient condition for the existence of M_1 and it is similar to Theorem 2. Note that the difference between “ $\forall i$ ” in Proposition 1 of [18] and “ $\exists i$ ” in Theorem 2 results from that Proposition 1 in [18] requires all groups of unknown states can be decided whether the states are identical.

Remark 1. Readers who are familiar with the problem of quantum state discrimination may find the conclusion of Theorem 2 is somewhat similar to the condition of mixed quantum state discrimination [6]. Actually, M_1 was constructed as a product of local discrimination of each state in the above proof of the sufficiency. However, this does not mean that a quantum comparison process must be always implemented by quantum state discrimination operations. In fact, a quantum comparison process acts on the composite Hilbert space $\mathcal{H}^{\otimes n}$ and is usually non-local, so it cannot be generally decomposed into several quantum state discrimination operations. Therefore, the necessity of the condition (8) cannot be straightforwardly derived from the known conclusions for the discrimination of mixed quantum state. In addition, Theorem 4 will explicitly show that on some occasions unambiguous quantum state discrimination can never be accomplished while unambiguous quantum state comparison can still succeed with non-zero probability.

Next, we study under what condition a quantum measurement can give the correct and conclusive result when the states are different, i.e., the existence of the measurement operator M_2 . It will be interesting to see that the existence of M_2 relies not only on the structure of the k states in the set, but also on n , the number of states to be compared. We first give a necessary condition for the existence of M_2 below.

Theorem 3. For unambiguous comparison of mixed quantum states, an unambiguous quantum measurement exists which can produce a conclusive result with a non-zero probability when the n states are actually different, i.e., a non-trivial M_2 exists, only if

$$\sum_{j \neq i} \text{Supp}(\sigma_j) \not\subseteq \text{Supp}(\sigma_i), \quad \forall i = 1, \dots, k. \quad (17)$$

Proof. We prove the theorem by contradiction. Assume $\sum_{j \neq i} \text{Supp}(\sigma_j) \subseteq \text{Supp}(\sigma_i)$ for some $i_0 \in \{1, \dots, k\}$, then

$$\text{Supp}(\sigma_j) \subseteq \text{Supp}(\sigma_{i_0}), \quad \forall j = 1, \dots, k, \quad (18)$$

so

$$\text{Supp}(\rho_1 \otimes \dots \otimes \rho_n) \subseteq \text{Supp}(\sigma_{i_0}^{\otimes n}), \quad (19)$$

where ρ_1, \dots, ρ_n are arbitrarily chosen from the k states in the candidate set. As M_2 is unambiguous, we have

$$\text{Tr}(M_2 \sigma_{i_0}^{\otimes n}) = 0. \quad (20)$$

Since $M_2 \geq 0$, Eq. (20) indicates that

$$\text{Supp}(\sigma_{i_0}^{\otimes n}) \perp \text{Supp}(M_2), \quad (21)$$

then with Eq. (19), the probability that M_2 occurs is

$$\text{Prob}(M_2) = \text{Tr}(M_2 \rho_1 \otimes \dots \otimes \rho_n) = 0 \quad (22)$$

for any n different states ρ_i ($i = 1, \dots, n$) chosen from the candidate set. ■

Remark 2. In Theorem 1, it has been shown that universal unambiguous comparison of mixed quantum states is impossible. In fact, Theorem 1 can be linked to Theorem 3 and derived from it. The universal comparison of mixed quantum states can be considered as a special case of unambiguous comparison of mixed states from a particular candidate set, i.e., the complete set of all mixed states. To derive Theorem 1 from Theorem 3, one only needs to note that the support of the mixed state $\frac{1}{d}I$ (d is the dimension of \mathcal{H}) is the whole Hilbert space \mathcal{H} and it certainly contains the support of any other mixed state, so the necessary condition in Theorem 3 is violated, leading to the impossibility of universal unambiguous comparison of mixed states.

It should be pointed out that Theorem 3 is a necessary condition but not a sufficient condition for the existence of M_2 . For example, suppose $k = 3$, and the three candidate states are

$$\sigma_1 = \frac{1}{2}(|\psi_1\rangle\langle\psi_1| + |\psi_2\rangle\langle\psi_2|), \sigma_2 = \frac{1}{2}(|\psi_2\rangle\langle\psi_2| + |\psi_3\rangle\langle\psi_3|), \sigma_3 = \frac{1}{2}(|\psi_1\rangle\langle\psi_1| + |\psi_3\rangle\langle\psi_3|), \quad (23)$$

where $|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle$ are orthogonal to each other. Apparently, these three candidate states satisfy the necessary condition (17), however, there is no way to produce a conclusive unambiguous result with a non-zero probability for any two different states chosen from (23): the support of M_2 must be orthogonal to the supports of $\sigma_1 \otimes \sigma_1, \sigma_2 \otimes \sigma_2, \sigma_3 \otimes \sigma_3$ due to the unambiguity of M_2 , but the sum of the supports of $\sigma_1 \otimes \sigma_1, \sigma_2 \otimes \sigma_2, \sigma_3 \otimes \sigma_3$ is the whole composite Hilbert space $\mathcal{H} \otimes \mathcal{H}$, so $M_2 = 0$ when $n = 2$. Thus, Eq. (17) is not sufficient for the existence of M_2 .

However, it is interesting to note that M_2 does exist for the above example when $n = 3$. In contrast to the case $n = 2$, when $n = 3$ we have

$$\text{Supp}(\sigma_1^{\otimes 3}) + \text{Supp}(\sigma_2^{\otimes 3}) + \text{Supp}(\sigma_3^{\otimes 3}) \neq \mathcal{H}^{\otimes 3} \quad (24)$$

and in fact,

$$|\psi_1\rangle \otimes |\psi_2\rangle \otimes |\psi_3\rangle \perp \text{Supp}(\sigma_1^{\otimes 3}) + \text{Supp}(\sigma_2^{\otimes 3}) + \text{Supp}(\sigma_3^{\otimes 3}), \quad (25)$$

therefore, M_2 can be constructed as the projector onto the subspace spanned by the state $|\psi_1\rangle \otimes |\psi_2\rangle \otimes |\psi_3\rangle$ and all permutations of its three factor states (e.g. $|\psi_2\rangle \otimes |\psi_3\rangle \otimes |\psi_1\rangle$ etc.), and this projector can unambiguously produce a conclusive result with a non-zero probability when the three states from the candidate set (23) are different.

From the above example one can see that whether it is possible to obtain an unambiguous result when the n unknown mixed states are different depends not only on the structures of the candidate states, but also on the number of states to be compared, i.e., n . One may wonder what value of n can make M_2 exist, if the candidate states already satisfy the necessary condition (17). The following interesting theorem answers this question.

Theorem 4. In the problem of unambiguous comparison of mixed quantum states, if $n \geq k$, then (17) is not only necessary but also sufficient for the existence of a non-trivial M_2 .

Proof. The necessity has been shown in Theorem 3, and we only need to prove the sufficiency here, provided $n \geq k$. The way to prove the sufficiency of (17) is to construct a non-trivial M_2 that can produce a conclusive result with a non-zero probability for at least one group of n different states.

Generally speaking, the comparison process is a non-local quantum measurement on the n states, and it seems not so easy to construct a qualified M_2 . Anyway, we can assume that M_2 can be decomposed into local measurements on the n states and explore whether such M_2 exists, and we finally find that such M_2 does exist.

Suppose

$$M_2 = P_1 \otimes \dots \otimes P_n, \quad (26)$$

where P_1, \dots, P_n are projectors performed on the n states respectively.

Let us remove any candidate state whose support is covered by the support of another candidate state (if the supports of several states are the same, then just keep one of them and remove the others), and denote the remaining states as $\sigma'_1, \dots, \sigma'_r$.

Since the measurement is unambiguous, when all the n states are identical, M_2 should never occur, i.e.,

$$\text{Prob}(M_2) = \text{Tr}(M_2 \sigma'_i \otimes \dots \otimes \sigma'_i) = \text{Tr}(P_1 \sigma'_i) \dots \text{Tr}(P_n \sigma'_i) = 0, \forall i = 1, \dots, r. \quad (27)$$

Now for $i = 1$, Eq. (27) can hold if one P_j satisfies $\text{Tr}(P_j \sigma'_1) = 0$, so one can choose $j = 1$ and then

$$P_1 = \text{Proj}(\text{Supp}^\perp(\sigma'_1)), \quad (28)$$

where $\text{Proj}(\text{Supp}^\perp(\sigma_1))$ denotes the projector onto the subspace $\text{Supp}^\perp(\sigma_1)$.

Similarly, let

$$P_2 = \text{Proj}(\text{Supp}^\perp(\sigma'_2)), P_3 = \text{Proj}(\text{Supp}^\perp(\sigma'_3)), \dots \quad (29)$$

then Eq. (27) can hold for $i = 2, \dots, r$.

It is easy to see that if such construction can be repeated for all σ'_i ($i = 1, \dots, r$), the unambiguity condition (27) can be satisfied by all σ'_i , and also by all the removed states because the support of any removed state is covered by one σ'_i ($i = 1, \dots, r$). Thanks to $n \geq k$, it is indeed possible to make the n projectors P_1, \dots, P_n run over

$$\text{Proj}(\text{Supp}^\perp(\sigma'_i)), \quad i = 1, \dots, r, \quad (30)$$

so M_2 can be constructed as

$$M_2 = \bigotimes_{i=1}^r \text{Proj}(\text{Supp}^\perp(\sigma'_i)) \otimes I^{\otimes(n-r)}. \quad (31)$$

Eq. (31) can ensure that M_2 is not trivial, because according to (17), for each σ_i there is at least one σ_{j_i} such that

$$\text{Supp}(\sigma_{j_i}) \not\subseteq \text{Supp}(\sigma_i), \quad (32)$$

and when the n states containing $\sigma_{j_1}, \dots, \sigma_{j_k}$, $\text{Prob}(M_2) > 0$. ■

Theorem 4 is quite interesting, because in a general quantum state comparison problem the number of the states chosen from a set can be varied and it is natural to think that the number of the chosen states may affect the possibility of the unambiguous comparison task. However, in previous literatures, no such conditions were found, and Theorem 4 is the first result to reveal the relation between the number of the states to be compared and the possibility of the unambiguous comparison task.

Remark 3. Theorem 4 shows the difference between the quantum state comparison problem and the quantum state discrimination problem. Eq. (17) is not a sufficient condition for unambiguous quantum state discrimination, so the states which satisfies (17) are necessary to be unambiguously distinguishable, but Theorem 4 tells that only if $n \geq k$, the states chosen from them can still be unambiguously compared when they are actually different. And Eq. (23) is such an example: apparently the states in Eq. (23) cannot be distinguished in an unambiguous way, but when $n = 3$, M_2 does exist indeed and it can be chosen as $\sum_{\text{Per} \in S} \text{Per}(|\psi_1\rangle\langle\psi_1| \otimes |\psi_2\rangle\langle\psi_2| \otimes |\psi_3\rangle\langle\psi_3|)$.

Next, we give another sufficient condition for the existence of M_2 which depends only on the structures of the candidate states, and this sufficient condition holds true for all $n \geq 2$.

Theorem 5. For unambiguous comparison of mixed quantum states, if the k candidate states $\sigma_1, \dots, \sigma_k$ satisfy (17) and the following condition

$$\text{Supp}(\sigma_{i_0}) \not\subseteq \sum_{j \neq i_0} \text{Supp}(\sigma_j), \quad \exists i_0 \in \{1, \dots, k\}, \quad (33)$$

then a non-trivial M_2 exists.

Proof. Like the proof of the last theorem, we construct a proper M_2 starting from a product of local projectors on the n states to be compared to prove this theorem.

Suppose

$$M_2 = P_1 \otimes \dots \otimes P_n, \quad (34)$$

where P_1, \dots, P_n are projectors on the n states respectively. Since the measurement is unambiguous, when $\rho_1 = \dots = \rho_n = \sigma_{i_0}$, M_2 should never produce a conclusive result, implying

$$\text{Prob}(M_2) = \text{Tr}(M_2 \sigma_{i_0} \otimes \dots \otimes \sigma_{i_0}) = \text{Tr}(P_1 \sigma_{i_0}) \dots \text{Tr}(P_n \sigma_{i_0}) = 0, \quad (35)$$

so one can let $P_1 = \text{Proj}(\text{Supp}^\perp(\sigma_{i_0}))$ and thus Eq. (35) is met for σ_{i_0} . But such a method cannot be repeated for other $j \neq i_0$, because n may be smaller k and in this case P_1, \dots, P_n cannot cover all k projectors $\text{Proj}(\text{Supp}^\perp(\sigma_j))$, $j = 1, \dots, k$.

Nevertheless, we can use another method to construct proper P_2, \dots, P_n to ensure $\text{Prob}(M_2) = 0$ when $\rho_1 = \dots = \rho_n = \sigma_j$, $j \neq i_0$. Considering Eq. (33), we have

$$\text{Proj}\left(\sum_{j \neq i_0} \text{Supp}(\sigma_j)\right)^\perp \neq 0. \quad (36)$$

Note that

$$\text{Supp}(\sigma_l) \perp \left(\sum_{j \neq i_0} \text{Supp}(\sigma_j)\right)^\perp, \quad \forall l \neq i_0,$$

so

$$\text{Tr}\left(\sigma_l \text{Proj}\left(\sum_{j \neq i_0} \text{Supp}(\sigma_j)\right)^\perp\right) = 0, \quad \forall l \neq i_0. \quad (37)$$

Then if one of P_2, \dots, P_n , say P_2 , is $\text{Proj}\left(\sum_{j \neq i_0} \text{Supp}(\sigma_j)\right)^\perp$, the unambiguity requirement can be satisfied for all $\rho_1 = \dots = \rho_n = \sigma_j$, $j \neq i_0$. Thus, a proper M_2 can be constructed as follows,

$$M_2 = \text{Proj}(\text{Supp}^\perp(\sigma_{i_0})) \otimes \text{Proj}\left(\sum_{j \neq i_0} \text{Supp}(\sigma_j)\right)^\perp \otimes I^{\otimes(n-2)}. \quad (38)$$

And $\text{Prob}(M_2) \neq 0$ when ρ_1, \dots, ρ_n are different and contain σ_i , thus the non-triviality condition is also satisfied. ■

From Theorem 2 to Theorem 5, we have studied the possibility to unambiguously compare the n unknown states when the n states are the same or different separately. However, it is interesting to note that the sufficient condition (33) for M_2 is essentially the same as the necessary and sufficient condition (8) for M_1 , so we can combine Theorems 2, 3, 5, and obtain the following corollary on the possibility of an unambiguous quantum measurement which can deal with both cases that the states are the same and that the states are different.

Corollary 1. For the problem of unambiguous comparison of mixed quantum states from a given state set, an unambiguous measurement exists which can produce conclusive results in both cases that the n states are actually the same or different with a non-zero probability (i.e., non-trivial M_1 and M_2 exist simultaneously), if and only if the following two conditions are both satisfied

$$\begin{aligned} \text{i.} \quad & \sum_{j \neq i} \text{Supp}(\sigma_j) \not\subseteq \text{Supp}(\sigma_i), \quad \forall i = 1, \dots, k; \\ \text{ii.} \quad & \text{Supp}(\sigma_i) \not\subseteq \sum_{j \neq i} \text{Supp}(\sigma_j), \quad \exists i \in \{1, \dots, k\}. \end{aligned} \quad (39)$$

It is worth pointing out that most previous researches on the quantum state comparison problem dealt with the two cases that the n states are the same or different separately, and most conclusions were also separate for these two cases. Corollary 1 is the first unified necessary and sufficient condition to deal with both two cases simultaneously.

V. CONCLUSION

In summary, we have studied the problem of comparing mixed quantum states in this article. Two types of state comparison are covered: universal comparison of mixed quantum states, and unambiguous comparison of mixed states

chosen from a given state set. The universal comparison of mixed quantum states is shown to be generally impossible, in marked contrast to the universal comparison of pure quantum states. The problem of comparing mixed states from a given set is divided into two parts: the condition for obtaining an unambiguous result when the states to be compared are actually the same and the condition when the states to be compared are actually different. We obtain a necessary and sufficient condition for the first case, and a necessary condition and two sufficient conditions for the second. An interesting theorem is derived for the necessary condition of the second case to be sufficient dependent on the relation between the number of the states to be compared and the number of the states in the candidate set. Furthermore, we find a unified necessary and sufficient condition for the the existence of an unambiguous quantum measurement which can be effective in both cases.

Comparison of mixed quantum states is an interesting and important problem since it can be used in various quantum verification applications like the quantum digital signature protocol, quantum fingerprinting, and so on. We hope our work could contribute to a deeper understanding and further solution to this problem.

ACKNOWLEDGEMENT

This work is supported by the NNSF of China (Grant No. 11075148), the CUSF, the CAS and the National Fundamental Research Program. S. Pang also acknowledges the support from the Innovation Foundation of USTC.

-
- [1] I. D. Ivanovic, Phys. Lett. A **123**, 257 (1987)
 - [2] D. Dieks, Phys. Lett. A **126**, 303 (1988)
 - [3] A. Peres, Phys. Lett. A **128**, 19 (1988)
 - [4] A. Chefles, Phys. Lett. A **239**, 339 (1998)
 - [5] L. M. Duan and G. C. Guo, Phys. Rev. Lett. **80**, 4999 (1998)
 - [6] Y. Feng, R. Duan and M. Ying, Phys. Rev. A **70**, 012308 (2004)
 - [7] S. Pang and S. Wu, Phys. Rev. A **80**, 052320 (2009)
 - [8] M. F. Sacchi, Phys. Rev. A, **71**, 062340 (2005)
 - [9] R. Duan, Y. Feng, and M. Ying, Phys. Rev. Lett, **98**, 100503 (2007)
 - [10] L. Li and D. Qiu, J. Phys. A: Math. Theor. **41**, 335302 (2008)
 - [11] R. Duan, Y. Feng, and M. Ying, Phys. Rev. Lett. **103**, 210501 (2009)
 - [12] M. Piani and J. Watrous, Phys. Rev. Lett. **102**, 250501 (2009)
 - [13] C.H. Bennett and S.J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992)
 - [14] A. K. Pati, P. Parashar and P. Agrawal, Phys. Rev. A **72**, 012329 (2005)
 - [15] S. M. Barnett, A. Chefles, and I. Jex, Phys. Lett. A **307**, 189 (2003)
 - [16] A. Chefles, E. Andersson, and I. Jex, J. Phys. A **37**, 7315 (2004)
 - [17] I. Jex, E. Andersson and A. Chefles, J. Mod. Opt. **51**, 505 (2004)
 - [18] M. Kleinmann, H. Kampermann, and D. Bruss, Phys. Rev. A **72**, 032308 (2005)
 - [19] Michal Sedlak, Mário Ziman, Vladimír Bužek, and Mark Hillery, Phys. Rev. A **77**, 042304 (2008)
 - [20] E. Andersson, M. Curty, and I. Jex, Phys. Rev. A **74**, 022304 (2006)
 - [21] H. Buhrman, R. Cleve, J. Watrous and R. de Wolf, Phys. Rev. Lett. **87**, 167902 (2001)
 - [22] S. Massar, Phys. Rev. A **71**, 012310 (2005)
 - [23] D. Gottesman and I. L. Chuang, arxiv: quant-ph/0105032 (2001)
 - [24] G. Zeng and C. H. Keitel, Phys. Rev. A **65**, 042312 (2002)
 - [25] Q. Li, W. H. Chan, and D.-Y. Long, Phys. Rev. A **79**, 054307 (2009)
 - [26] E. Kashefi, A. Kent, V. Vedral, and K. Banaszek, Phys. Rev. A **65**, 050304(R) (2002)
 - [27] Michal Sedlak and M. Ziman, Phys. Rev. A **79**, 012303 (2009)
 - [28] M. Ziman, T. Heinosaari, and M. Sedlak, Phys. Rev. A **80**, 052102 (2009)